

PATENT
81942.0008
Express Mail Label No. EL 713 695 985 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Yasuyuki MURAKAMI

Serial No: Not assigned

Filed: January 23, 2001

For: SECRET KEY GENERATING METHOD,
ENCRYPTION METHOD, CRYPTOGRAPHIC
COMMUNICATION METHOD AND
CRYPTOGRAPHIC COMMUNICATION
SYSTEM

Art Unit: Not assigned

Examiner: Not assigned

jc760 U.S. PTO
09/768130
01/23/01

TRANSMITTAL OF PRIORITY DOCUMENT

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

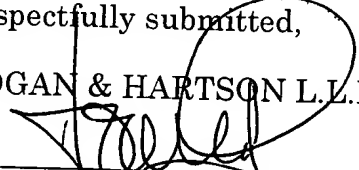
Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 2000-016358 which was filed January 25, 2000, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,
HOGAN & HARTSON L.L.P.

Date: January 23, 2001

By: 
Louis A. Mok
Registration No. 22,585
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2000年 1月25日

出 願 番 号
Application Number: 特願2000-016358

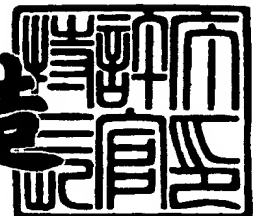
出 願 人
Applicant(s): 村田機械株式会社
笠原 正雄



2000年 8月18日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3064842

【書類名】 特許願

【整理番号】 20875

【提出日】 平成12年 1月25日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00
H04L 9/00

【発明の名称】 秘密鍵生成方法，暗号化方法及び暗号通信方法

【請求項の数】 3

【発明者】

【住所又は居所】 京都府京都市伏見区竹田向代町 1 3 6 番地 村田機械株式会社 本社工場内

【氏名】 村上 恭通

【特許出願人】

【識別番号】 000006297

【氏名又は名称】 村田機械株式会社

【代表者】 村田 純一

【特許出願人】

【識別番号】 597008636

【氏名又は名称】 笠原 正雄

【復代理人】

【識別番号】 100114557

【弁理士】

【氏名又は名称】 河野 英仁

【電話番号】 06-6944-4141

【代理人】

【識別番号】 100078868

【弁理士】

【氏名又は名称】 河野 登夫

【電話番号】 06-6944-4141

【手数料の表示】

【予納台帳番号】 001889

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9805283

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 秘密鍵生成方法、暗号化方法及び暗号通信方法

【特許請求の範囲】

【請求項 1】 複数のセンタの夫々にて、エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎に設定された複数ビットのハッシュ値とを用いて、前記エンティティ固有の秘密鍵を生成する方法において、所定の複数ビット列から各センタ毎に複数の任意の順位のものを選択することにより前記ハッシュ値を各センタ毎に設定することを特徴とする秘密鍵生成方法。

【請求項 2】 複数のセンタの夫々にて、各エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎に設定された複数ビットのハッシュ値とを用いて、各エンティティ固有の秘密鍵を生成し、この秘密鍵に含まれている、暗号文の送信先である相手のエンティティに対応する成分を使用して生成した共通鍵を用いて平文を暗号文に暗号化する暗号化方法において、所定の複数ビット列から各センタ毎に複数の任意の順位のものを選択することにより前記ハッシュ値を各センタ毎に設定することを特徴とする暗号化方法。

【請求項 3】 センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵から求めた共通鍵を用いて平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を、前記センタから送付された該エンティティ固有の秘密鍵から求めた、前記共通鍵と同一の共通鍵を用いて元の平文に復号することにより、エンティティ間で情報の通信を行うこととし、前記センタが複数設けられており、その複数のセンタ夫々は、各エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎に設定された複数ビットのハッシュ値とを用いて、各エンティティ固有の秘密鍵を生成し、各エンティティは、自身固有の秘密鍵に含まれている、相手のエンティティに対応する成分を使用して前記共通鍵を生成するようにした暗号通信方法において、所定の複数ビット列から各センタ毎に複数の任意の順位のものを選択することにより前記ハッシュ値を各センタ毎に設定することを特徴とする暗号通信方法。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、センタにてエンティティ固有の秘密鍵を生成する秘密鍵生成方法、情報の内容が当事者以外にはわからないように情報を暗号化する暗号化方法、及び、暗号文にて通信を行う暗号通信方法に関する。

【 0 0 0 2 】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」、「マルチアクセス」、「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事、外交面で用いられてきた暗号技術が注目されている。

【 0 0 0 3 】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【 0 0 0 4 】

暗号化鍵と復号鍵とは、等しくても良いし、異なっても良い。両者の鍵が等しい暗号系は、共通鍵暗号系と呼ばれ、米国商務省標準局が採用したDES（Data Encryption Standards）はその典型例である。また、両者の鍵が異なる暗号

系の一例として、公開鍵暗号系と呼ばれる暗号系が提案された。この公開鍵暗号系は、暗号系を利用する各ユーザ（エンティティ）が暗号化鍵と復号鍵とを一対ずつ作成し、暗号化鍵を公開鍵リストにて公開し、復号鍵のみを秘密に保持するという暗号系である。公開鍵暗号系では、この一対となる暗号化鍵と復号鍵とが異なり、一方向性関数を利用することによって暗号化鍵から復号鍵を割り出せないという特徴を持たせている。

【 0 0 0 5 】

公開鍵暗号系は、暗号化鍵を公開するという画期的な暗号系であって、高度情報化社会の確立に必要な上述した 3 つの要素に適合するものであり、情報通信技術の分野等での利用を図るべく、その研究が活発に行われ、典型的な公開鍵暗号系として R S A 暗号系が提案された。この R S A 暗号系は、一方向性関数として素因数分解の困難さを利用して実現されている。また、離散対数問題を解くことの困難さ（離散対数問題）を利用した公開鍵暗号系も種々の手法が提案されてきた。

【 0 0 0 6 】

また、各エンティティの住所、氏名等の個人を特定する I D (Identity) 情報を利用する暗号系が提案された。この暗号系では、I D 情報に基づいて送受信者間で共通の暗号化鍵を生成する。また、この I D 情報に基づく暗号技法には、（1）暗号文通信に先立って送受信者間での予備通信を必要とする方式と、（2）暗号文通信に先立って送受信者間での予備通信を必要としない方式とがある。特に、（2）の手法は予備通信が不要であるので、エンティティの利便性が高く、将来の暗号系の中樞をなすものと考えられている。

【 0 0 0 7 】

この（2）の手法による暗号系は、I D - N I K S (ID-based non-interactive key sharing scheme) と呼ばれており、通信相手の I D 情報を用いて予備通信を行うことなく暗号化鍵を共有する方式を採用している。I D - N I K S は、送受信者間で公開鍵、秘密鍵を交換する必要がなく、また鍵のリスト及び第三者によるサービスも必要としない方式であり、任意のエンティティ間で安全に通信を行える。

【0008】

図5は、このID-NIKSのシステムの原理を示す図である。信頼できるセンタの存在を仮定し、このセンタを中心にして共通鍵生成システムを構成している。図5において、エンティティXの特定情報であるエンティティXの名前、住所、電話番号等のID情報は、ハッシュ関数 $h(\cdot)$ を用いて $h(ID_X)$ で表す。センタは任意のエンティティXに対して、センタ公開情報 $\{PC_i\}$ 、センタ秘密情報 $\{SC_i\}$ 及びエンティティXのID情報 $h(ID_X)$ に基づいて、以下のように秘密情報 S_{Xi} を計算し、秘密裏にエンティティXへ配布する。

$$S_{Xi} = F_i(\{SC_i\}, \{PC_i\}, h(ID_X))$$

【0009】

エンティティXは他の任意のエンティティYとの間で、暗号化、復号のための共通鍵 K_{XY} を、エンティティX自身の秘密情報 $\{S_{Xi}\}$ 、センタ公開情報 $\{PC_i\}$ 及び相手先のエンティティYのID情報 $h(ID_Y)$ を用いて以下のように生成する。

$$K_{XY} = f(\{S_{Xi}\}, \{PC_i\}, h(ID_Y))$$

また、エンティティYも同様にエンティティXへの鍵を共通鍵 K_{YX} を生成する。もし常に $K_{XY} = K_{YX}$ の関係が成立すれば、この鍵 K_{XY} 、 K_{YX} をエンティティX、Y間で暗号化鍵、復号鍵として使用できる。

【0010】

上述した公開鍵暗号系では、例えばRSA暗号系の場合にその公開鍵の長さは現在の電話番号の十数倍となり、極めて煩雑である。これに対して、ID-NIKSでは、各ID情報を名簿という形式で登録しておけば、この名簿を参照して任意のエンティティとの間で共通鍵を生成することができる。従って、図5に示すようなID-NIKSのシステムが安全に実現されれば、多数のエンティティが加入するコンピュータネットワーク上で便利な暗号系を構築できる。このような理由により、ID-NIKSが将来の暗号系の中心になると期待されている。

【0011】

このID-NIKSには、次のような2つの問題点がある。一つは、センタがBig Brotherとなる（すべてのエンティティの秘密を握っており、Key Escrow S

system になってしまう) 点である。もう一つは、ある数のエンティティが結託するとセンタの秘密を演算できる可能性がある点である。この結託問題については、これを計算量的に回避するための工夫が多数なされているが、完全な解決は困難である。

【 0 0 1 2 】

この結託問題の難しさは、特定情報 (ID 情報) に基づく秘密パラメータがセンタ秘密と個人秘密との二重構造になっていることに起因する。ID-NIKS では、センタの公開パラメータと個人の公開された特定情報 (ID 情報) とこの 2 種類の秘密パラメータとにて暗号系が構成され、しかも各エンティティが各自に配布された個人秘密を見せ合ってもセンタ秘密が露呈されないようにする必要がある。よって、その暗号系の構築の実現には解決すべき課題が多い。

【 0 0 1 3 】

そこで、本発明者等は、特定情報 (ID 情報) をいくつか分割し、複数のセンタの夫々からその分割した特定情報 (ID 情報) に基づくすべての秘密鍵をエンティティに配布することにより、数学的構造を最小限に抑えることができ、結託問題の回避を可能にし、その暗号系の構築が容易である ID-NIKS による秘密鍵生成方法、暗号化方法及び暗号通信方法 (以下、これらを先行例という) を提案している。

【 0 0 1 4 】

結託問題を解決することを目的として提案されてきたエンティティの特定情報 (ID 情報) に基づく種々の暗号系が不成功となった理由は、エンティティの結託情報からセンタ秘密を割り出せないようにするための工夫を数学的構造に求め過ぎていたためである。数学的構造が複雑過ぎると、安全性を証明するための方法も困難となる。そこで、先行例の提案方法では、エンティティの特定情報 (ID 情報) をいくつか分割し、分割した各特定情報 (ID 情報) についてすべての秘密鍵をエンティティに配布することにより、数学的構造を最小限に抑えるようにする。

【 0 0 1 5 】

先行例では、信頼される複数のセンタが設けられ、各センタは各エンティティ

の分割した各特定情報（ID情報）に対応する数学的構造を持たない秘密鍵を夫々生成して、各エンティティへ送付する。各エンティティは、各センタから送られてきたこれらの秘密鍵と通信相手の公開されている特定情報（ID情報）とから共通鍵を、予備通信を行わずに生成する。よって、すべてのエンティティの秘密を1つのセンタが握るようなことはなく、各センタがBig Brother にならない。

【0016】

【発明が解決しようとする課題】

そして、本発明者等は、このような先行例の改良を研究しており、その先行例を適用した暗号通信システムの構築を図っている。このような暗号通信システムにとっては、センタの数を増やすことにより安全性を向上することができる。従って、ある数のセンタにて実際に構築されている暗号通信システムに対して更なる新規のセンタを追加することが頻繁に行われると考えられる。

【0017】

新規のセンタを暗号通信システムに追加参入させる度に、既存のセンタ及び新規のセンタに新しいハッシュ値を設定して全体の新しいハッシュ関数系を構築しなければならず、システム全体の変更が避けられない。システム全体を変更せずに、新規のセンタの追加に対応するためには、各センタが独自のハッシュ関数を公開する、予め十分に長いビット長のハッシュ関数を設定しておくなどの対策が考えられる。しかしながら、前者の対策では各エンティティが新たなハッシュ関数を鍵共有ソフトウェアに組み込むことが容易ではない、後者の対策ではいくら長いビット長のハッシュ関数を準備しておいてもセンタの追加数には限界があるという問題がある。

【0018】

本発明は斯かる事情に鑑みてなされたものであり、新規のセンタを追加した場合においても既存のセンタのハッシュ値を変更する必要がなく、安全性を向上しながら多数の新規のセンタを容易に追加することができる秘密鍵生成方法、暗号化方法及び暗号通信方法を提供することを目的とする。

【0019】

【課題を解決するための手段】

請求項 1 に係る秘密鍵生成方法は、複数のセンタの夫々にて、エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎に設定された複数ビットのハッシュ値とを用いて、前記エンティティ固有の秘密鍵を生成する方法において、所定の複数ビット列から各センタ毎に複数の任意の順位のものを選択することにより前記ハッシュ値を各センタ毎に設定することを特徴とする。

【0020】

請求項 2 に係る暗号化方法は、複数のセンタの夫々にて、各エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎に設定された複数ビットのハッシュ値とを用いて、各エンティティ固有の秘密鍵を生成し、この秘密鍵に含まれている、暗号文の送信先である相手のエンティティに対応する成分を使用して生成した共通鍵を用いて平文を暗号文に暗号化する暗号化方法において、所定の複数ビット列から各センタ毎に複数の任意の順位のものを選択することにより前記ハッシュ値を各センタ毎に設定することを特徴とする。

【0021】

請求項 3 に係る暗号通信方法は、センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵から求めた共通鍵を用いて平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を、前記センタから送付された該エンティティ固有の秘密鍵から求めた、前記共通鍵と同一の共通鍵を用いて元の平文に復号することにより、エンティティ間で情報の通信を行うこととし、前記センタが複数設けられており、その複数のセンタ夫々は、各エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎に設定された複数ビットのハッシュ値とを用いて、各エンティティ固有の秘密鍵を生成し、各エンティティは、自身固有の秘密鍵に含まれている、相手のエンティティに対応する成分を使用して前記共通鍵を生成するようにした暗号通信方法において、所定の複数ビット列から各センタ毎に複数の任意の順位のものを選択することにより前記ハッシュ値を各センタ毎に設定することを特徴とする。

【0022】

本発明では、所定の複数ビット列からなる原ハッシュ値列から各センタ毎に複数の任意の順位のビットを選択して、選択した複数ビットを各センタ毎のハッシュ値として設定する。このようにすることにより、既存の各センタに複数ビットのハッシュ値が設定されていても、それらのハッシュ値を変更することなく、新規のセンタについて、原ハッシュ値列から選択した複数ビットにて、既存の各センタとは異なるハッシュ値を設定することができる。よって、既存の各センタのハッシュ値を変えることなく、多数の新規のセンタをID-NIKSによる暗号通信システムに容易に追加することが可能となる。

【0023】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図1は、本発明の暗号通信システムの構成を示す模式図である。情報の隠匿を信頼できる複数（J個）のセンタ1が設定されており、これらのセンタ1としては、例えば社会の公的機関を該当できる。

【0024】

これらの各センタ1と、この暗号通信システムを利用するユーザとしての複数の各エンティティ a, b, \dots, z とは、通信路 $2_{a1}, \dots, 2_{aJ}, 2_{b1}, \dots, 2_{bJ}, \dots, 2_{z1}, \dots, 2_{zJ}$ により接続されており、これらの通信路を介して各センタ1から各エンティティ固有の秘密鍵が各エンティティ a, b, \dots, z へ伝送されるようになっている。また、2人のエンティティの間には通信路 $3_{ab}, 3_{az}, 3_{bz}, \dots$ が設けられており、この通信路 $3_{ab}, 3_{az}, 3_{bz}, \dots$ を介して通信情報を暗号化した暗号文が互いのエンティティ間で伝送されるようになっている。

【0025】

各エンティティの氏名、住所などを示す特定情報であるIDベクトルをL次元2進ベクトルとし、図2に示すようにそのIDベクトルをブロックサイズ M_1, M_2, \dots, M_J 毎にJ個のブロックに分割する。例えば、エンティティ i のIDベクトル（ベクトル I_i ）を下記（1）のように分割する。分割特定情報である各ベクトル I_{ij} ($j=1, 2, \dots, J$) をID分割ベクトルと呼ぶ。ここで、 $M_j=M$ とすると、全てのID分割ベクトルのサイズが等しくなる。また

、 $M_j = 1$ と設定することも可能である。なお、各エンティティの公開 ID ベクトルはハッシュ関数により、 L ビットに変換される。

【0026】

【数 1】

$$\vec{I}_i = [\vec{I}_{i1} | \vec{I}_{i2} | \cdots | \vec{I}_{iJ}] \quad \cdots (1)$$

【0027】

(センタ 1 での準備処理)

センタ 1 は以下の公開鍵及び秘密鍵を準備し、公開鍵を公開する。

公開鍵	P	大きな素数
	J	ID ベクトルの分割ブロック数
	M_j	分割した ID ベクトルのサイズ ($j = 1, 2, \dots, J$)
	L	ID ベクトルのサイズ ($L = M_1 + M_2 + \dots + M_J$)
秘密鍵	g	$GF(P)$ の原始元
	H_j	乱数からなる $2^{M_j} \times 2^{M_j}$ の対称行列 ($j = 1, 2, \dots, J$)
	α_{ij}	エンティティ i の個人秘密乱数 (但し、 $\alpha_{i1} \alpha_{i2} \cdots \alpha_{iK} \equiv 1 \pmod{P-1}$)

【0028】

(エンティティの登録処理)

エンティティ i に登録を依頼された各センタ 1 は、準備した鍵とエンティティ i の J 個の ID 分割ベクトルについて、それぞれに対応する J 個の秘密鍵ベクトル s_{ij} ($j = 1, 2, \dots, J$) を以下の式 (2-1), (2-2), \dots , (2- J) に従って求め、求めたベクトル s_{ij} を秘密裏に送って、登録を完了する。

【0029】

【数 2】

$$\overrightarrow{s_{i1}} \equiv g^{\alpha_{i1} H_1 [\overrightarrow{I_{i1}}]} \pmod{P} \quad \dots (2-1)$$

$$\overrightarrow{s_{i2}} \equiv \alpha_{i2} H_2 [\overrightarrow{I_{i2}}] \pmod{P-1} \quad \dots (2-2)$$

$$\vdots$$

$$\overrightarrow{s_{iJ}} \equiv \alpha_{iJ} H_J [\overrightarrow{I_{iJ}}] \pmod{P-1} \quad \dots (2-J)$$

【0030】

但し、 g をスカラー、 A 、 B を行列とした場合、 $B = g^A$ は A の各 (μ, ν) 成分について g のべき乗を行うことを表す。即ち、式 (3) のようになる。また、 H_j [ベクトル I_{ij}] は対称行列 H_j からベクトル I_{ij} に対応した行を 1 行抜き出したものを表し、 $[\cdot]$ の操作を参照と定義する。

【0031】

【数 3】

$$B_{\mu\nu} = g^{A_{\mu\nu}} \quad \dots (3)$$

【0032】

(エンティティ間の共通鍵の生成処理)

エンティティ i は、自身の秘密鍵ベクトル s_{i1} の中から、エンティティ m の I 分割ベクトルであるベクトル I_{m1} に対応する成分のベクトル s_{i1} [ベクトル I_{m1}] を選び出し、また、 $j = 2, \dots, J$ の各ブロックについて秘密鍵ベクトル s_{ij} の中から、ベクトル I_{mj} に対応する成分のベクトル s_{ij} [ベクトル I_{mj}] を各ブロック毎に選び出す。そして、 P を法とし、ベクトル s_{i1} [ベクトル I_{m1}] を底として残りのすべてのベクトル s_{ij} [ベクトル I_{mj}] ($j = 2, \dots, J$) を順次べき乗することにより、共通鍵 K_{im} を求める。この K_{im} を求める演算式は具体的に式 (4) となり、この K_{im} はエンティティ m 側から求めた共通鍵 K_{mi} と一致する。

【0033】

【数 4】

$$\begin{aligned}
 J_{im} &\equiv \overrightarrow{s_{i1}} [\overrightarrow{I_{m1}}] \overrightarrow{s_{i2}} [\overrightarrow{I_{m2}}] \cdots \overrightarrow{s_{iJ}} [\overrightarrow{I_{mJ}}] \\
 &\equiv g^{\alpha_{i1} \cdots \alpha_{iJ}} H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] \cdots H_J [\overrightarrow{I_{iJ}}] [\overrightarrow{I_{mJ}}] \\
 &\equiv g^{H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] \cdots H_J [\overrightarrow{I_{iJ}}] [\overrightarrow{I_{mJ}}]} \pmod{P}
 \end{aligned}$$

・・・(4)

【0034】

次に、上述した暗号システムにおけるエンティティ間の情報の通信について説明する。図3は、2人のエンティティa, b間における情報の通信状態を示す模式図である。図3の例は、エンティティaが平文（メッセージ）Mを暗号文Cに暗号化してそれをエンティティbへ伝送し、エンティティbがその暗号文Cを元の平文（メッセージ）Mに復号する場合を示している。

【0035】

j (j=1, 2, ..., J) 番目のセンタ1には、各エンティティa, b固有のベクトル s_{aj} , s_{bj} （秘密鍵）を前記式(2-j)に従って求める秘密鍵生成器1aが備えられている。そして、各エンティティa, bから登録が依頼されると、そのエンティティa, bの秘密鍵ベクトル s_{aj} , s_{bj} がエンティティa, bへ送付される。

【0036】

エンティティa側には、J個の各センタ1から送られる固有の秘密鍵ベクトル s_{a1} , ..., s_{aj} , ..., s_{aJ} をテーブル形式で格納しているメモリ10と、これらの秘密鍵ベクトルの中からエンティティbに対応する成分であるベクトル s_{a1} [ベクトル I_{b1}] , ..., ベクトル s_{aj} [ベクトル I_{bj}] , ..., ベクトル s_{aJ} [ベクトル I_{bJ}] を選び出す成分選出器11と、選び出されたこれらの成分を使用してエンティティaが求めるエンティティbとの共通鍵 K_{ab} を生成する共通鍵生成器12と、共通鍵 K_{ab} を用いて平文（メッセージ）Mを暗号文Cに暗号化して通信

路 30 へ出力する暗号化器 13 とが備えられている。

【0037】

また、エンティティ b 側には、各センタ 1 から送られる固有の秘密鍵ベクトル $s_{b1}, \dots, s_{bj}, \dots, s_{bJ}$ をテーブル形式で格納しているメモリ 20 と、これらの秘密鍵ベクトルの中からエンティティ a に対応する成分であるベクトル s_{b1} [ベクトル I_{a1}] , ..., ベクトル s_{bj} [ベクトル I_{aj}] , ..., ベクトル s_{bJ} [ベクトル I_{aJ}] を選び出す成分選出器 21 と、選び出されたこれらの成分を使用してエンティティ b が求めるエンティティ a との共通鍵 K_{ba} を生成する共通鍵生成器 22 と、共通鍵 K_{ba} を用いて通信路 30 から入力した暗号文 C を平文（メッセージ）M に復号して出力する復号器 23 とが備えられている。

【0038】

エンティティ a からエンティティ b へ情報を伝送しようとする場合、まず、各センタ 1 で式 (2-1), (2-2), ..., (2-J) に従って求められて、予めメモリ 10 に格納されている秘密鍵ベクトル $s_{a1}, s_{a2}, \dots, s_{aJ}$ が成分選出器 11 へ読み出される。そして、成分選出器 11 にて、エンティティ b に対応する成分であるベクトル s_{a1} [ベクトル I_{b1}] , ベクトル s_{a2} [ベクトル I_{b2}] , ..., ベクトル s_{aJ} [ベクトル I_{bJ}] が選び出されて共通鍵生成器 12 へ送られる。共通鍵生成器 12 にて、これらの成分を使用して式 (4) に従って共通鍵 K_{ab} が求められ、暗号化器 13 へ送られる。暗号化器 13 において、この共通鍵 K_{ab} を用いて平文（メッセージ）M が暗号文 C に暗号化され、暗号文 C が通信路 30 を介して伝送される。

【0039】

通信路 30 を伝送された暗号文 C はエンティティ b の復号器 23 へ入力される。各センタ 1 で式 (2-1), (2-2), ..., (2-J) に従って求められて、予めメモリ 20 に格納されている秘密鍵ベクトル $s_{b1}, s_{b2}, \dots, s_{bJ}$ が成分選出器 21 へ読み出される。そして、成分選出器 21 にて、エンティティ a に対応する成分であるベクトル s_{b1} [ベクトル I_{a1}] , ベクトル s_{b2} [ベクトル I_{a2}] , ..., ベクトル s_{bJ} [ベクトル I_{aJ}] が選び出されて共通鍵生成器 22 へ送られる。共通鍵生成器 22 にて、これらの成分を使用して式 (4) に従って共通鍵 K_{ba} が求めら

れ、復号器 2 3 へ送られる。復号器 2 3 において、この共通鍵 K_{ba} を用いて暗号文 C が平文（メッセージ） M に復号される。

【 0 0 4 0 】

ここで、本発明の特徴部分である各センタ 1 でのハッシュ値の設定について説明する。以下の例では、図 1 に示したような暗号通信システムにおいて、4 個（ $J = 4$ ）のセンタ 1 が既存しており、これに新たに別の 1 または複数のセンタ 1 を追加する場合を考える。なお、各センタ 1 に設定するハッシュ値は 1 0 ビットとする。

【 0 0 4 1 】

4 個の新規のセンタ 1 を追加する場合に、各 1 0 ビットずつの新しいハッシュ値を設定することになるが、従来では、全 8 個のセンタ 1 に対して 8 0 ビットの新しいハッシュ関数系を構築するようにしている。よって、この場合には、既存のセンタ 1 のハッシュ値が変更されることになる。このように、従来では、新規のセンタを暗号通信システムに追加させる度に、ハッシュ値設定の面倒な処理を行わなければならない。

【 0 0 4 2 】

本発明では、次のようにして、追加した各センタ 1 の新しいハッシュ値を設定する。既存の 4 個の各センタ 1 におけるハッシュ値を並べたデータ列を所定の 4 0 ビットの原ハッシュ値列（例えば、1 番目のセンタ 1 でのハッシュ値が順位 1 ～ 1 0 番目のビット、また、2 番目、3 番目、4 番目のセンタ 1 でのハッシュ値が夫々順位 1 1 ～ 2 0 番目、2 1 ～ 3 0 番目、3 1 ～ 4 0 番目のビットとした構成）とし、新規の各センタ 1 毎に、その所定の 4 0 ビットの原ハッシュ値列から既存の各センタ 1 での組合せと同じにならないように複数の任意の順位のビットを 1 0 個選択して、選択した複数ビットをそのセンタ 1 のハッシュ値として設定する。例えば、この 4 0 ビットの原ハッシュ値列から、1 番目、3 番目、8 番目、1 0 番目、1 6 番目、2 1 番目、2 2 番目、2 7 番目、3 3 番目、3 5 番目のビットを選択してハッシュ値として設定する。このようなビットの選択パターンは ${}_{40}C_{10}$ 通りあり、非常に多数のセンタ 1 の追加に対応できる。

【 0 0 4 3 】

従って、本発明では、既存の４個の各センタ１におけるハッシュ値を変更することなく、新規追加の４個の各センタ１におけるハッシュ値を設定することができる。新規のセンタ１を追加した場合でも、ハッシュ関数系を設計し直す必要がない。よって、安全性を上げながら、極めて容易に多数の新規のセンタ１を追加することが可能である。

【 0 0 4 4 】

図４は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するプログラムは、各センタ１において各エンティティのＩＤベクトルとハッシュ値とを用いて各エンティティ固有の秘密鍵を生成する処理を含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ４０は、各センタ１側に設けられている。

【 0 0 4 5 】

図４において、コンピュータ４０とオンライン接続する記録媒体４１は、コンピュータ４０の設置場所から隔たって設置される例えばWWW(World Wide Web)のサーバコンピュータを用いてなり、記録媒体４１には前述の如きプログラム４１aが記録されている。記録媒体４１から読み出されたプログラム４１aがコンピュータ４０を制御することにより、各センタ１において各エンティティ固有の秘密鍵を生成する。

【 0 0 4 6 】

コンピュータ４０の内部に設けられた記録媒体４２は、内蔵設置される例えばハードディスクドライブまたはROMなどを用いてなり、記録媒体４２には前述の如きプログラム４２aが記録されている。記録媒体４２から読み出されたプログラム４２aがコンピュータ４０を制御することにより、各センタ１において各エンティティ固有の秘密鍵を生成する。

【 0 0 4 7 】

コンピュータ４０に設けられたディスクドライブ４０aに装填して使用される記録媒体４３は、運搬可能な例えば光磁気ディスク、CD-ROMまたはフレキシブルディスクなどを用いてなり、記録媒体４３には前述の如きプログラム４３aが記録されている。記録媒体４３から読み出されたプログラム４３aがコンピ

ユーザ 40 を制御することにより、各センタ 1 において各エンティティ固有の秘密鍵を生成する。

【 0 0 4 8 】

【発明の効果】

以上詳述したように、本発明では、所定の複数ビット列から各センタ毎に複数の任意の順位のビットを選択することにより各センタ毎のハッシュ値を設定するようにしたので、既存のセンタのハッシュ値を変更することなく、新規のセンタについて、既存の各センタとは異なるハッシュ値を簡便に設定することができ、多数の新規のセンタを I D - N I K S による暗号通信システムに容易に追加することが可能である。

【 0 0 4 9 】

(付記)

なお、以上の説明に対して更に以下の項を開示する。

(1) 送信すべき情報である平文を暗号文に暗号化する暗号化处理、及び、送信された暗号文を元の平文に復号する復号処理を、複数のエンティティ間で相互に行うこととし、各エンティティの特定情報を複数のブロックに分割した分割特定情報と各センタ毎に設定された複数ビットのハッシュ値とを用いて、各エンティティ固有の秘密鍵を生成して各エンティティへ送付する複数のセンタと、該センタから送付された自身の秘密鍵と通信対象のエンティティの特定情報に基づく公開鍵とを利用して前記暗号化处理及び復号処理に用いる共通鍵を生成する複数のエンティティとを有する暗号通信システムにおいて、所定の複数ビット列から各センタ毎に複数の任意の順位のものを選択することにより前記ハッシュ値を各センタ毎に設定するようにした暗号通信システム。

(2) 第(1)項の暗号通信システムであって、新規のセンタを既存の複数のセンタに追加した際に、前記既存の複数のセンタに設定されているハッシュ値を並べた原ハッシュ値列から任意の順位のものを選択することにより前記新規のセンタのハッシュ値を設定するようにした暗号通信システム。

(3) コンピュータに、エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎に設定された複数ビットのハッシュ値とを用いて、

前記エンティティ固有の秘密鍵を生成させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、所定の複数ビット列から複数の任意の順位のものを選択することにより前記ハッシュ値を設定することをコンピュータに実行させるプログラムコード手段を含むプログラムが記録されている記録媒体。

【図面の簡単な説明】

【図 1】

本発明の暗号通信システムの構成を示す模式図である。

【図 2】

エンティティの ID ベクトルの分割例を示す模式図である。

【図 3】

2 人のエンティティ間における情報の通信状態を示す模式図である。

【図 4】

記録媒体の実施の形態の構成を示す図である。

【図 5】

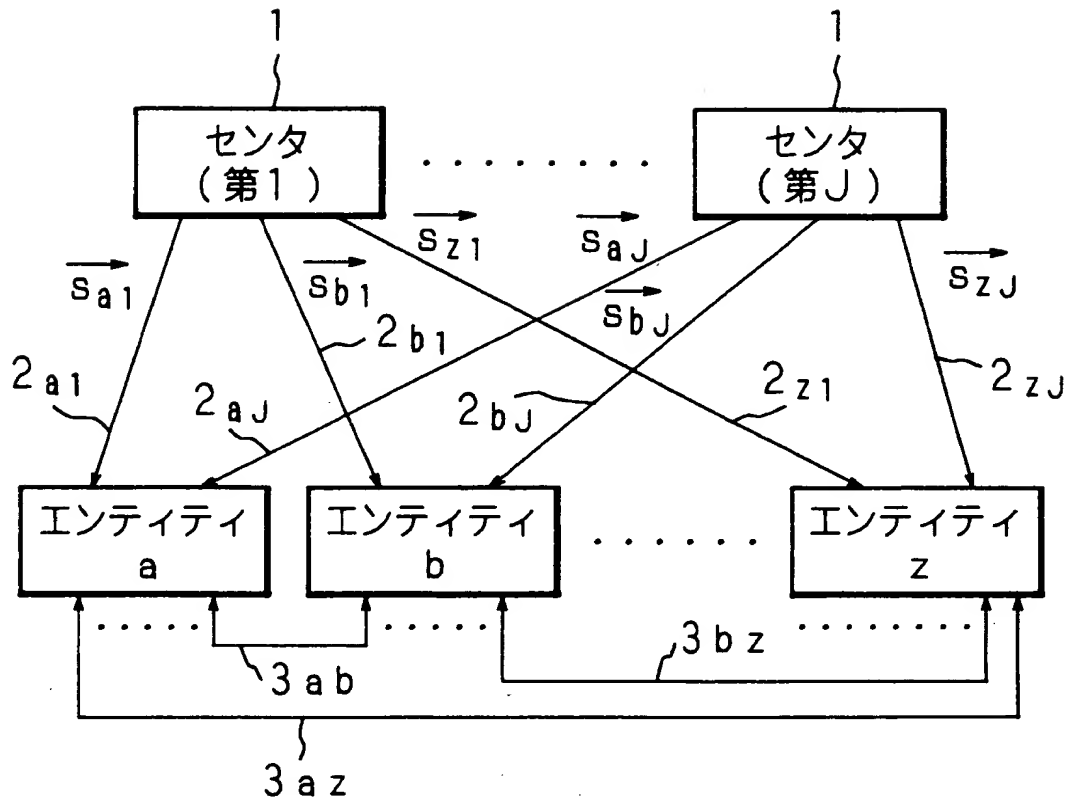
ID-NIKS のシステムの原理構成図である。

【符号の説明】

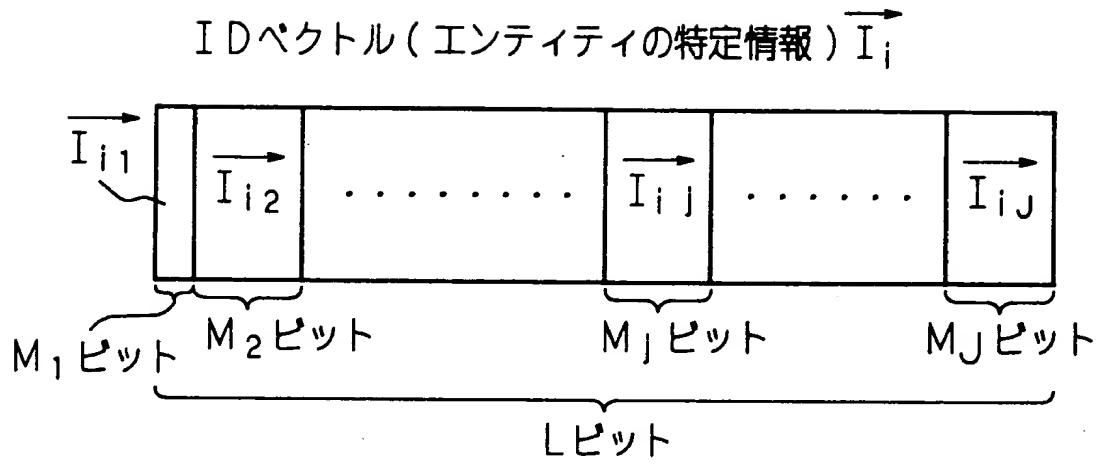
- 1 センタ
- 1 a 秘密鍵生成器
- 1 0, 2 0 メモリ
- 1 1, 2 1 成分選出器
- 1 2, 2 2 共通鍵生成器
- 1 3 暗号化器
- 2 3 復号器
- 3 0 通信路
- 4 0 コンピュータ
- 4 1, 4 2, 4 3 記録媒体

【書類名】 図面

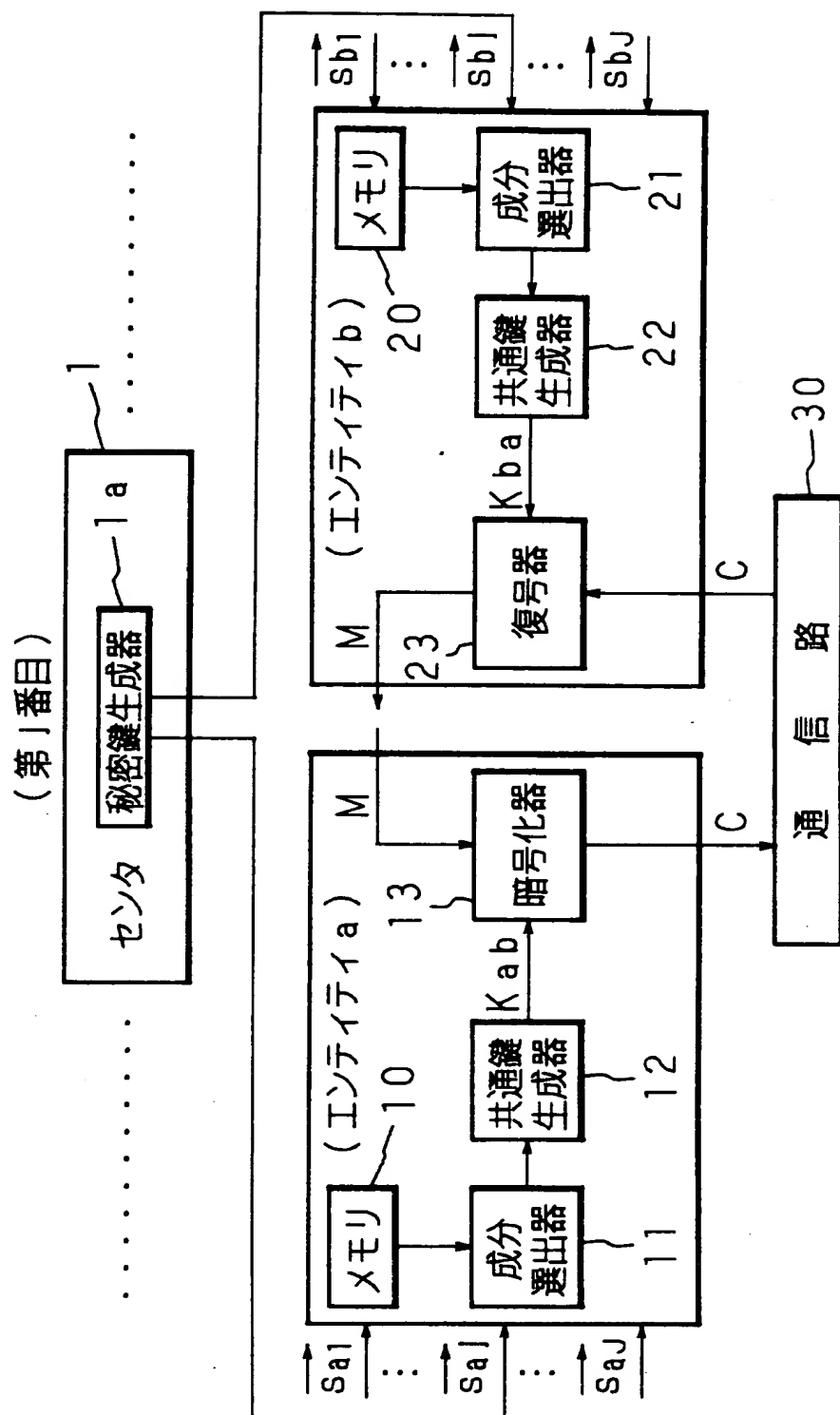
【図 1】



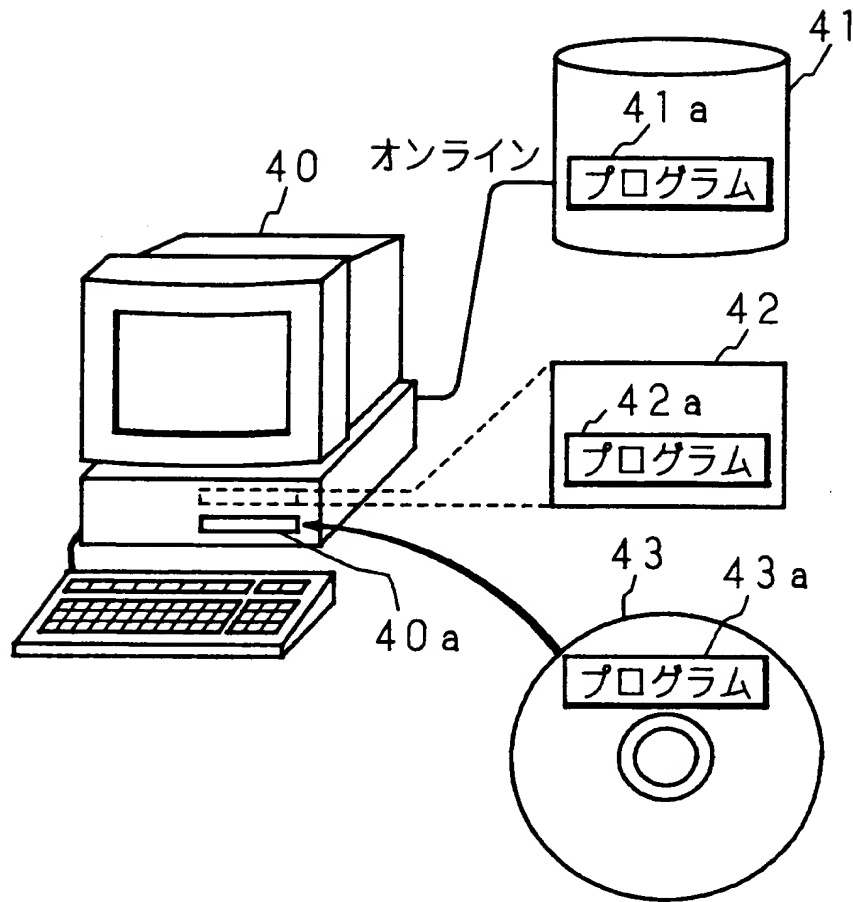
【図 2】



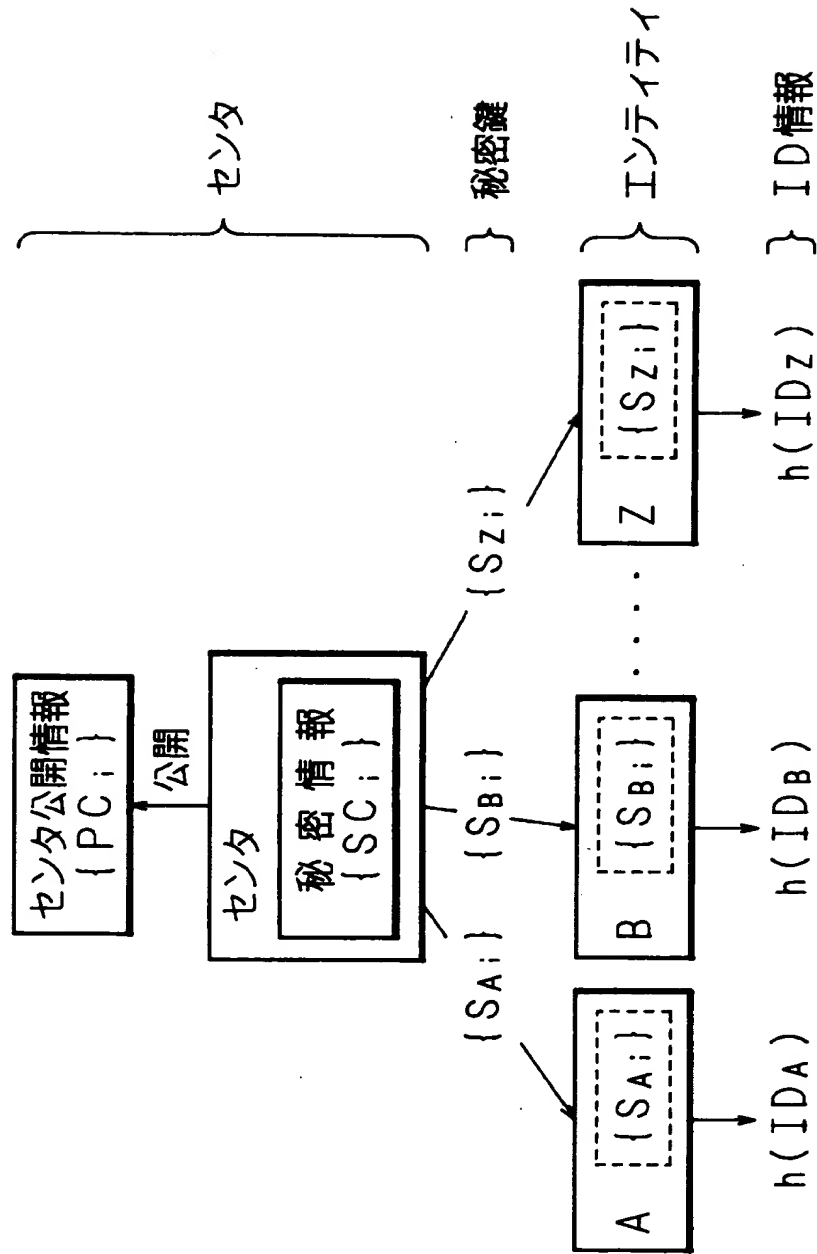
【図 3】



【図 4】



【図 5】



【書類名】 要約書

【要約】

【課題】 I D - N I K S 暗号通信システムにあって、安全性を向上しながら新規のセンタを容易に追加できる秘密鍵生成方法、暗号化方法及び暗号通信方法を提供することを目的とする。

【解決手段】 各センタ 1 にて、各エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎に設定された複数ビットのハッシュ値とを用いて、各エンティティ固有の秘密鍵を生成する。所定の複数ビット列からなる原ハッシュ値列から各センタ 1 毎に複数の任意の番目のビットを選択して各センタ 1 毎のハッシュ値を設定する。新規のセンタ 1 を既存の複数のセンタ 1 に追加した際に、既存の複数のセンタ 1 に設定されているハッシュ値を並べた原ハッシュ値列から任意の番目のものを選択することにより、既存の複数のセンタ 1 のハッシュ値を変えないで、新規のセンタ 1 のハッシュ値を設定する。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2000-016358
受付番号	50000073737
書類名	特許願
担当官	塩崎 博子 1606
作成日	平成12年 7月12日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000006297
【住所又は居所】	京都府京都市南区吉祥院南落合町3番地
【氏名又は名称】	村田機械株式会社

【特許出願人】

【識別番号】	597008636
【住所又は居所】	大阪府箕面市栗生外院4丁目15番3号
【氏名又は名称】	笠原 正雄

【復代理人】

【識別番号】	100114557
【住所又は居所】	大阪府大阪市中央区釣鐘町二丁目4番3号 河野 特許事務所
【氏名又は名称】	河野 英仁

【代理人】

申請人	
【識別番号】	100078868
【住所又は居所】	大阪府大阪市中央区釣鐘町二丁目4番3号 河野 特許事務所
【氏名又は名称】	河野 登夫

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 6 2 9 7]

1. 変更年月日	1 9 9 0 年 8 月 7 日
[変更理由]	新規登録
住 所	京都府京都市南区吉祥院南落合町 3 番地
氏 名	村田機械株式会社

出 願 人 履 歴 情 報

識別番号 [597008636]

1. 変更年月日 1997年 1月21日
[変更理由] 新規登録
住 所 大阪府箕面市栗生外院4丁目15番3号
氏 名 笠原 正雄